IN THE CLAIMS

The listing of the claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) An access control method performed by an access control system, including:

receiving an access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said access request;

applying an access rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system, wherein verifying said identification data corresponds to a first level of access control; and

applying at least one additional different level of access control following a predetermined number of failed attempts to verify said identification data by said user of said apparatus, including invoking sequentially the different levels of access control depending on the number of failed attempts to verify said identification data by said user for access requests over predetermined periods of time.

2. (Currently Amended) An access control method as claimed in Claim 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol and said at least one additional level of access control includes blocking all access requests by said data processing apparatus, and wherein said detecting is a second level of access control, said sending of said communication software and execution of said additional communication protocol is a third level of access control, and said blocking is a fourth level of access control.

3. (Previously Presented) An access control method as claimed in Claim 1, wherein said identification data is a random unique security code; and

said apparatus is sent a unique identification number for the apparatus, for sending with subsequent access requests and which expires if the security code is not verified within a predetermined period of time.

4. (Previously Presented) An access control method as claimed in Claim 1, wherein said identification data is verified by contacting an independent communications device with a known association to said user and said data processing apparatus, and having said user provide said identification data using said device.

5. (Previously Presented) An access control method as claimed in Claim 1, wherein said identification data is verified by said access control system by receiving said identification data from said user using an independent communication means having a known association to said user and said data processing apparatus.

6. (Previously Presented) An access control method as claimed in Claim 3, wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user.

7. (Previously Presented) An access control method as claimed in Claim 1, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.

8. (Original) An access control method as claimed in Claim 7, wherein said communication software encrypts said access requests.

9. (Previously Presented) An access control method as claimed in Claim 2, wherein said blocking involves denying all access requests that include address data or said unique identification number that corresponds to said data processing apparatus.

10. (Currently Amended) An access control method performed by an access control system, including:

receiving an access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said access request, wherein said identification data is a random unique security code, and said apparatus is sent a unique identification number for the apparatus, for sending with subsequent access requests and which expires if the security code is not verified within a predetermined period of time;

applying an access rate limit for verifying access to said service, using an access request queue, until said identification data is received from a user of said apparatus and verified by said access control system, wherein verifying said identification data corresponds to a first level of access control; and

applying at least one additional different level of access control following a predetermined number of failed attempts to verify said identification data by said user of said apparatus;

wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user, and said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol, and wherein said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

11. (Previously Presented) An access control method as claimed in Claim 10, wherein said at least one additional level of access control includes a fourth level of access control involving blocking all access requests by said data processing apparatus.

12. (Previously Presented) An access control method as claimed in Claim 11, wherein said blocking involves denying all access requests that include address data or said unique identification number that corresponds to said data processing apparatus.

13. (Original) An access control method as claimed in Claim 12, wherein the address data is an IP address or segment.

14. (Previously Presented) An access control method executed by a computer system, including:

invoking a first control level applying an access rate limit, using an access request queue, and attempting to verify said user;

invoking a second control level applying hack program detection tests to said access requests and attempting to verify said user;

invoking a third control level requiring use of predetermined download software for transmitting said access requests and attempting to verify said user;

invoking a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and

invoking said control levels sequentially depending on a number of failed attempts to verify said user;

wherein attempting to verify said user comprises sending unique identification data to said user, receiving identification data from said user in response to the sent identification data, and verifying the received identification data.

15. (Previously Presented) An access control method as claimed in Claim 14, wherein said user is verified by contacting an independent communications device with a known association to said user and said data processing apparatus, and having said user provide identification data using said device.

16. (Original) An access control system having components for executing the steps of the access control method as claimed in Claim 1.

17. (Original) Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in Claim 1.

18. (Previously Presented) An access control system, including:

an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server, using an access request queue, until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and

an interactive voice response system for contacting an independent communications device having an association with said user and said data processing apparatus, issuing a request for said identification data, and providing the identification data received from said user in response to said request to said access server in order to verify said user.

19. (Previously Presented) An access control method as claimed in Claim 4 or 15, wherein said independent device is a telephone of the user.

20. (Previously Presented) An access control method as claimed in Claim 5, wherein said independent communications means is a telephone of the user.

21. (Previously Presented) An access control method as claimed in Claim 1, wherein

said unique identification data is sent in a graphic format and received from said user in a different format.

22. (Previously Presented) An access control method as claimed in Claim 6, wherein said detecting includes sending the unique identification data in a graphic format, and requesting a response in a different format.

23. (Previously Presented) An access control method as claimed in Claim 11, wherein said blocking is at a router level close to said apparatus.

24. (Currently Amended) An access control system as claimed in Claim 18, ~~whereas~~wherein said independent device is a telephone of said user.

25. (Previously Presented) The access control method of Claim 1, wherein the step of applying the access rate limit for verifying access to said service comprises placing the access request in the access request queue when the rate limit is exceeded.

26. (Previously Presented) The access control method of Claim 1, wherein the access rate limit limits a number of access requests from said data processing apparatus over a period of time, until said user of said apparatus sends said unique identification data, and said unique identification data is verified.

27. (Previously Presented) The access control method of Claim 14, wherein the rate limit limits a number of access requests from said data processing apparatus over a period of time, until said user of said apparatus sends said unique identification data, and said unique identification data is verified.

28. (Previously Presented) The access control method of Claim 18, wherein the rate limit limits a number of access requests from said data processing apparatus over a period of time, until said user of said apparatus sends said unique identification data, and said unique identification data is verified.